Department of Energy
Cyber Security Awards Criteria

To foster continued excellence in the Department of Energy (DOE) cyber security environment, the Office of the Chief Information Officer (OCIO) has developed an awards program to recognize those DOE Federal and contractor employees who have made significant contributions, both managerial and technical, to the Department's Cyber Security Program. In addition, these individuals have demonstrated a continued commitment to excellence in protecting critical information assets, as well as developing and/or implementing emerging security technologies within the DOE complex. The OCIO views the Cyber Security Awards Program as a vital part of its comprehensive outreach effort – an effort to effectively communicate the mission, goals, requirements, and accomplishments of the Department.

Four different Cyber Security awards are given annually to any DOE employee. Typically, these awards are presented during DOE cyber security conferences or workshops. Additionally, DOE cyber security professionals are recognized for successfully obtaining professional certifications in the cyber security arena. The cyber awards are detailed below.

Outstanding Cyber Contribution to DOE/Charlene Douglass Award

This award is presented to an individual who exhibits the highest level of dedication, contributory effort, and cyber security expertise within the Department. This individual is also a continuous advocate for cyber security initiatives in his/her organization and in other Federal forums. This award is given in remembrance of Charlene Douglass – a well-known computer security pioneer who effectively managed the cyber security program at Los Alamos National Laboratory for 30 years. Her strategic vision and collaborative efforts with other DOE security professionals helped create the foundation for the DOE Cyber Security Program in practice today.

Required Selection Criteria:

1. The individual must have at least 10 years of cyber security experience. Experience in the Federal government and private industry will be considered.

2. The individual must have at least five years of managerial experience in a cyber organization. This experience can include any level of management as long as the individual was responsible for managing the work effort of a cyber staff or a group of employees supporting a cyber initiative. These positions can include, but are not limited to, CSSMs, ISSMs, CSPMs, DAAs, program managers, project managers, team leaders, etc.

Additional Selection Criteria – potential candidate must meet four out of the seven criteria listed below:

1. Sustained leadership, vision, and direction in implementing the Department's cyber security initiatives.

2. Continuous advocate for Department-wide cyber security initiatives in his/her specific organization and in other Federal forums.

3. Demonstrated expertise in cyber security technologies.

4. Significant contribution to all aspects of an organization's cyber security program to include management and oversight, technical implementation, administrative procedures, and user training and awareness.

5. Significant contribution to all aspects of the Department's cyber security initiatives to include organizational programmatic implementations, policy review and development, assistance with strategic direction, etc.

6. Actively pursue innovative approaches to enhance cyber security practices where needed or to streamline where appropriate.

7. Participate in complex-wide collaborative efforts to share information and to consider/research technological advancements made by other agencies.

Superior Leadership

This award is presented to an individual who has demonstrated excellence in his/her ability to effectively manage a cyber security initiative or program with well-informed insight and uncompromising integrity. In addition to being a leader, this individual is an innovator with the proven ability to proactively implement technological changes in a variety of information technology and security platforms.

Required Selection Criteria:

1. The individual must have at least five years of cyber security experience. Experience in the Federal government and private industry will be considered.

2. The individual must have at least three years of managerial experience in a cyber organization. This experience can include any level of management as long as the individual was responsible for managing the work effort of a cyber staff or a group of employees supporting a cyber initiative. These positions can include, but are not limited to, CSSMs, ISSMs, CSPMs, DAAs, program managers, project managers, team leaders, etc.

Additional Selection Criteria – potential candidate must meet three out of the five criteria listed below:

1. Sustained leadership, vision, and direction in implementing the Department's cyber security initiatives.

2. Innovatively implement and manage new technologies to better meet an organization's mission or to improve a current business process by significantly reducing costs or eliminating redundancy.

3. Successfully implement new policy via standard project management practices that ensure timely implementation of new requirements, elimination of legacy requirements and procedures, elimination of redundant processes, etc.

4. Fully supports and provides experienced insight to all aspects of the organization's cyber security program to include policy implementation and compliance, technical implementations, employee training, and user training and awareness initiatives.

5. Design and implement an effective performance measurement program that assesses organizational compliance with cyber security requirements.

Innovative Technical Achievement

This award is presented to an individual (or team) who has demonstrated creativity, initiative, and technical excellence in developing and successfully implementing a new technology or solution that enhances the security of an enterprise or site information technology system. This individual (or team) is also an advocate for collaborating with other DOE sites and Federal agencies in an effort to share emerging or proven technologies that protect information assets.

Selection Criteria – potential candidate or team must meet three out of the five criteria listed below:

1. Develop and/or implement new technologies that enhance the security of network architectures, specialized computing tools, legacy systems, multi-site communication platforms, etc.

2. Develop and/or implement innovative new cyber security technologies to better meet an organization's mission.

3. Demonstrates expertise in design, development, and implementation of information technology solutions or when resolving technical installation problems with such solutions that meet cyber security initiatives or requirements.

4. Implement or contribute to other notable technology initiatives that significantly enhance the security posture of an organization or the Department.

5. Participate in a multi-site initiative to research, develop, and deploy an enhanced security technology that benefits the complex.

Cyber Security Training and Awareness

This award is presented to an individual (or team) that has demonstrated significant achievements in cyber security training and/or awareness by implementing or utilizing innovative training and awareness approaches that convey Department-specific requirements for key personnel as well as integrate National security guidance.

Selection Criteria – potential candidate or team must meet three out of the five criteria listed below:

1. Develop and/or implement new training technologies, either electronic or via class instruction, that integrate National guidance and role-based requirements.

2. Develop and/or implement an electronic-based training solution that benefits multiple organizations.

3. Effectively use commercially-available training and awareness tools to realize cost efficiencies.

4. Develop and deploy innovated approaches to enhance cyber security user awareness training.

5. Implement or contribute to other notable achievements that significantly improve the quality of the Department's training and awareness initiative.

Program Guidelines

Any DOE employee can nominate an individual for an award, including themselves. However, nominations may be submitted for only one of the awards described above. Multiple nominations will be returned to the submission author.

A team of employees can be nominated for an award except for the *Outstanding Contribution/Charlene Douglass Award* and the *Superior Leadership Award*. Team nominations must be limited to 15 team members.

Qualifying technical implementations (e.g., new security technology, access control process shared by multiple sites, etc.) or business processes must be formally approved and in production. Individuals or teams responsible for proposed implementations can be submitted for consideration in the year that the implementation/technology is formally approved.

A potential recipient or team must meet the minimum number of selection criteria as documented for a specific award. It is the author's responsibility to fully document how the potential recipient or team has met the criteria. Supporting documentation must be limited to two pages.

All award submissions must be Unclassified.

DOE employees must use the official award nomination forms included in this document. The form is also electronically posted on the OCIO web site, http://cio.energy.gov. Submissions that are not completed using the official form will be returned to the author without formal consideration.

Selection Process

The acceptable time frame for submitting nominations will be announced on an annual basis via the following methods (at a minimum): broadcast messages on DOECAST; formal notification to the Cyber Security Working Group (CSWG); publication on the OCIO web site, etc.

Award recipients will be chosen by a committee of Senior DOE Cyber Security professionals. The Office of Cyber Security is responsible for coordinating the selection committee.

A numerical rating system will be used to evaluate selection criteria. For additional questions concerning how an individual or team is selected for these awards, please contact Sue Farrand at 202-586-2514.

In addition to public recognition during a cyber security conference or workshop, award recipients will receive a token of appreciation. These tokens can be plaques, lapel pins, framed certificates, etc. The type of token will vary each year.

All nomination forms must be submitted electronically by the posted due date to susan.farrand@hq.doe.gov .

Late submissions will be returned to the author without formal consideration.

Contact Information

All questions concerning the OCIO awards program can be directed to the Cyber Security Mailbox at cyber.security@hq.doe.gov or directly to Sue Farrand at susan.farrand@hq.doe.gov or 202-586-2514. All nominations must be submitted to susan.farrand@hq.doe.gov .

This document, the nomination form, and due date for the current award year can be found at http://cio.energy.gov.

OCIO CYBER SECURITY AWARDS NOMINATION FORM

Due date for submission: ______________

I. *Nominee Information*

Name of Nominee:____
Title of Nominee:____
Site Location of Nominee:____

Please note: If nominating a team for an award, please attach a sheet to this form that details each team member's name, title, and site location.
Team nominations can only be submitted for the *Innovative Technical Achievement* and *Cyber Security Training and Awareness* awards. No more than 15 names can be submitted for an award. It is the author's responsibility to only recognize the major contributors to the project/initiative.

II. *Nominator Information*

Date of Submission:____
Your Name:____
Your Title:____
Site Location:____
Contact Number or e-mail:____

III. Cyber *Security Award*

Check one award for consideration.

( ) Outstanding Cyber Contribution to DOE/Charlene Douglass Award
( ) Superior Leadership
( ) Innovative Technical Achievement
( ) Cyber Security Training and Awareness

IV. *Nomination Requirements*

Provide a brief synopsis of the candidate's (or team) qualifications, significant contributions, successful technical and/or program implementations, etc., that satisfy the selection criteria as documented for each award.

OCIO CYBER SECURITY AWARDS NOMINATION FORM
Due date for submission: ______________

The nominator is responsible for thoroughly documenting how the recipient or team has met the minimum number of qualifying criteria. **Please limit supporting documentation to no more than two additional typed pages, or less than 500 words.**

Note: If you are submitting a nominee for the *Outstanding Cyber Contribution to DOE/Charlene Douglass Award* or for the *Superior Leadership Award*, the nominee must meet the **required selection criteria** as noted for each award. Tenure requirements for a potential recipient must be documented in the supporting documentation.

Tenure Requirements (if applicable):

Description of Qualifying Selection Criteria (if needed, two additional pages of supporting documentation can be included):

Send an electronic copy of this form and any supporting documentation to susan.farrand@hq.doe.gov.